HENFIELD PARISH COUNCIL INFORMATION TECHNOLOGY POLICY

Purpose of the IT Policy

The purpose of an IT policy is to establish clear parameters for how councillors, staff, and other authorised users use council-provided technology or equipment in the course of their duties.

Scope of this policy

This policy applies to all councillors, staff, and other authorised users, regardless of their working location or pattern, including those who are home-based, office-based, or work on a flexible or part-time basis. It sets out the expectations for the appropriate use of IT equipment and systems provided by the council.

Computer use

Hardware

1.1.1 Henfield Parish Council computer equipment is provided for council purposes only. However reasonable personal use is permitted (reasonable interpreted in the opinion of the Clerk). Any personal use of our computers and systems should not interrupt our daily council work in any way.

1.1.2 Locking computers when leaving desk, staff, and other authorised users must lock their computers when leaving their desks to prevent unauthorised access.

1.1.3 Equipment should not be dismantled or reassembled without seeking advice.

1.1.4 Any faults or necessary repairs must be reported to The Clerk

2.1 Portable equipment

2.1.1 Portable equipment includes laptop computers, netbooks, tablets, mobile and smart phones with email capability and access to the internet etc.

2.1.2 All portable computers must be stored safely and securely when not in use in the office, i.e. when travelling or when working from home. Portable equipment (unless locked in a secure cabinet or office) should be kept with or near the user at all times; should not be left unattended when away from council premises and should never be left in parked vehicles or at any council or non-council premises.

2.1.3 Multi-Factor Authentication (MFA) is a security process that requires users to verify their identity using two or more independent methods— and is enabled on Parish Council staff equipment

2.2 Use of own devices

2.2.1 Personal laptops and other computers or other devices should not be brought into work and used to access council IT systems during working hours, unless this has been authorised by the employee's line manager. This is to ensure that no viruses enter the system, to prevent time being wasted during working hours on personal use and to assist in maintaining security, confidentiality, and data protection.

2.2.2 . Any emails sent from own devices should be sent from a council email account and should not identify the individual's personal email address.

2.2.3 Councillors, staff, and other authorised persons that use council systems are expected to use all devices in an ethical and respectful manner and in accordance with this policy.

2.2.4 In cases of legal proceedings against the council , the council may need to temporarily take possession of a device, whether council-owned or personal to retrieve the relevant data.

2.2.5 Wherever possible the user should maintain a clear separation between the personal data processed on the council's behalf and that processed for their own personal use, for example, by using different apps for council and personal use. If the device supports both work and personal profiles, the work profile must always be used for work-related purposes.

2.2.6 Councillors, staff, and other authorised users who intend to use their own devices via the council's infrastructure must ensure that they:

- use a 6-digit pin, strong password to protect their device(s) from being accessed.
- always password protect any documents containing confidential information that are sent as attachments to an email, and notify the password separately (preferably by a means other than email).

2.2.7 Personal data relating to councillors, staff, and other authorised users, associates, residents, external stakeholders should not be saved to any personal accounts

2.2.8 Personal information and sensitive data should never be saved on councillors, staff, or other authorised users own devices as this may breach confidentiality agreements, especially if the device is used by other people from time to time.

2.2.9 If removable media are used to transfer data (e.g. USB drives or CDs), the user must also securely delete the data on the media once the transfer is complete.

2.2.10 Any work done on user's own equipment should be stored securely and password protected and should always be backed up in accordance with the council's standard backup procedures.

Password and Authentication Policy

3.1.1 All user accounts must be protected by strong, secure passwords.

In addition to strong passwords, Multi-Factor Authentication (MFA) is enabled for Parish Council staff.

3.1.2 Access to Passwords

- Passwords are personal and must not be shared under any circumstances.
- Only the assigned user of an account may access or use the associated password.
- In exceptional cases access to system credentials may be granted to authorised personnel from the IT provider with appropriate approvals and logging.
- Administrative credentials must be stored securely and only accessible to authorised personnel with a copy provided to the Chair and Vice Chair of Council, in a sealed envelope, only to be accessed in an emergency.

3.1.3 Password Storage and Management

- Passwords must not be stored in plain text or written down in insecure locations. Any passwords that are written down must be stored securely and not in public view.

3.1.4 Password Change Requirements

- Immediately change password if compromise is suspected.

3.1.5 Password Access Control and Logging

- All access to administrative or shared credentials must be logged and auditable.
- Attempts to access unauthorized passwords will be treated as a security incident.

3.1.6 Responsibility

- Users are responsible for creating and maintaining secure passwords for their accounts.

Remote working

4.1.1 Increased IT security measures apply to those who work away from their normal place of work (e.g. whilst travelling, working from home)

Papers, files or computer equipment must not be left unattended at non council premises unless arrangements have been made with The Clerk. Any data should be kept safely and should only be disposed of securely;

Email

5.1.1 Council email facilities are intended to promote effective and speedy communication on work-related matters. Councillors, staff, and other authorised users need to be careful not to introduce viruses onto council systems and should take proper account of the security advice.

5.1.2 All councillors, staff, and other authorised users who need to use email as part of their role will normally be given their own council email address and account. The council may, at any time, withdraw email access, should it feel that this is no longer necessary for the role or that the system is being abused.

5.1.3 Email messages sent on the council's account are for council use only. Personal use is not permitted.

Use of the Internet

6.1 Copyright

6.1.1 Much of what appears on the Internet is protected by copyright. Any copying without permission, including electronic copying, is illegal and therefore prohibited. The Copyright, Designs and Patents Act 1988 set out the rules. The copyright laws not only apply to documents but also to software. The infringement of the copyright of another person or organisation could lead to legal action being taken against the council and damages being awarded, as well as disciplinary action, including dismissal, being taken against the perpetrator.

6.1.2 It is easy to copy electronically, but this does not make it any less an offence. The council's policy is to comply with copyright laws, and not to bend the rules in any way.

6.1.3 Councillors, staff, and other authorised users should not assume that because a document or file is on the Internet, it can be freely copied.

6.2 Data Protection

6.2.1 Special rules apply to the processing of personal and sensitive personal data. For further guidance on this, see the council's data protection policy.

Use of social media

7.1.1 Social media includes blogs, Wikipedia and other similar sites where text can be posted; multimedia or user generated media sites (YouTube); social networking sites (such as Facebook. Care should be taken when using social media at any time, either using council systems or at home.

7.1.2 The council recognises the importance of councillors, staff, and other authorised users joining in and helping to shape sector conversation and enhancing its image through

blogging and interaction in social media. Therefore, where it is relevant to use social networking sites as part of the individual's position, this is acceptable.

However, inappropriate comments and postings can adversely affect the reputation of the council, even if it is not directly referenced. Therefore, even if the council is not named, care should be taken with any views expressed.

7.1.3 To protect both the council and its interests, everyone is required to comply with the following rules about social media, whether in relation to their council role or personal social networking sites, and irrespective of whether this is during or after working hours:

- Contacts from any of the council's databases should not be downloaded and connected with on LinkedIn or other social networking sites with electronic address book facilities, unless this has been authorised.
- Even if the council is not mentioned, care should be taken with any views expressed on social media sites and any views should clearly be stated to be the writer's own (e.g. via a disclaimer statement such as: "The comments and other content on this site are my own and do not represent the positions or opinions of my employer/ the council.") Writers must not claim or give the impression that they are speaking on behalf of the council.
- Any employee who is developing a site or writing a blog that will mention the council, council current or potential plans, councillors, or staff, must inform The Clerk that they are writing this and gain agreement before going 'live'.
- The council expects councillors, staff, and other authorised users to be respectful about the council and not to engage in any behaviour that will reflect negatively on its reputation.
- Comments posted by councillors, staff, and other authorised users on any sites should be knowledgeable, accurate and professional and should not compromise the council in any way.
- Councillors, staff, and other authorised users must be aware that they are personally liable for anything that they write or present online (including on an online forum or blog, post, feed or website). Councillors should always be mindful of the Members Code of Conduct and Nolan Principles. Employees may be subject to disciplinary action for comments, content, or images that are defamatory, embarrassing,
- Postings to websites or anywhere on the internet and social media of any kind, or in any press or media of any kind, should not breach copyright or other law or disclose confidential information, defame or make derogatory comments about the council ~~or~~

Misuse

Misuse of IT systems and equipment is not in line with the council's standards of conduct and will be taken seriously. Any inappropriate or unauthorised use may lead to formal action, including disciplinary proceedings or, in serious cases, dismissal.